Aug. 13 - We’ve been told since the dawn of the Internet that the e-mail we send and receive on company time is fair game for our employers to monitor. Many took for granted, though, that e-mail sent from private accounts was just that: private. How naive.

As if hacking worries weren’t enough, two recent legal developments have raised further fears among Web privacy advocates in the United States. In one case, the Federal Communications Commission voted 5-0 last week to prohibit businesses from offering broadband or Internet phone service unless they provide Uncle Sam with backdoors for wiretapping access. And in a separate decision last month, a federal appeals court decided that e-mail and other electronic communications are not protected under a strict reading of wiretap laws. Taken together, these decisions may make it both legally and technologically easier to wiretap Internet communications, some legal experts told NEWSWEEK. “All the trends are toward easier to tap,” says Kevin Bankston, an attorney at the nonprofit Electronic Frontier Foundation.

The FCC’s plans to require Internet-based phone and broadband services to be engineered for easy wiretapping is a response to a request from the FBI and other law-enforcement agencies. The proposal would bring Internet-based phone providers in line with the Communications Assistance for Law Enforcement Act (CALEA), which requires “telecommunications” carriers to make their networks wiretap-friendly. The FCC says the government must still go through all of the necessary legal steps to obtain the authority to wiretap; CALEA simply makes it technologically easier to do. “This will not have an effect on whether there is appropriate lawful authority—that remains the same,” says FCC spokesman Julius Knapp. “All this really is addressing is whether the carrier is required to have the capability to provide the information that’s covered by a court order.”

Then there’s U.S. v. Councilman. In January 1998, an online bookseller called Interloc offered e-mail accounts to its dealer clients. The idea was that by secretly copying messages Interloc customers received from rival Amazon.com, the booksellers could gain a market advantage. Totally illegal, right? Not according to the federal court of appeals decision. Bradford C. Councilman, then an Interloc supervisor, claimed he was innocent of wiretapping because the law did not apply: since the messages had been stored on Interloc’s servers while they were being processed, they were not intercepted in transit. The court agreed with this literal reading of the wiretap laws. “We believe that the language of the statute makes clear that Congress meant to give lesser protection to electronic communications than wire and oral communication,” the court wrote in its decision. Under a 1986 amendment to the 1968 Wiretap Act, companies are banned from monitoring customer communications—but not from reading stored customer communications.

Is this outrageous? “This difference between stored communications and more transitory [communications] is a pretty refined one that really was ill-fitting at the time it was passed,” says Jonathan Zittrain, codirector of Harvard Law School’s Berkman Center for Internet and
Society. "It's even worse now." The framers of the law, he says, wanted to make it harder to conduct ongoing surveillance than undertake a one-time intrusion. "The Councilman decision sort of puts that on its end, because it says you can do a series of one-shot intrusions that amount to the same as surveillance—but still treat it as merely a one-shot deal." The Department of Justice, which prosecuted the case, did not return NEWSWEEK's calls asking for comment.

As it is, the wiretap laws have exceptions for the interception of unencrypted or unscrambled radio signals. So any easy-to-intercept e-mail you may send from your Wi-Fi-enabled laptop at your friendly neighborhood coffee shop is treated as a radio signal and therefore may not have the same protections under the law that wire and oral communications do. When the EFF's Bankston looks at the FCC ruling side by side with Councilman, he sees the former as making it technologically easier to wiretap Internet communications and the latter as lowering legal barriers. "Building the infrastructure for a surveillance state is not good public hygiene," he quips.

Not all lawyers see the situation in such bleak terms. Susan Crawford, an assistant professor at New York's Cardozo Law School who writes extensively on the FCC, isn't quite buying this conspiracy theory. "I'm not convinced that either Councilman or CALEA changes any individual's privacy online," she says. She does, however, agree that the Councilman case highlighted a weakness in the current law, adding that the recent developments could be seen "as part of the trend at the FBI and the Department of Justice and the Drug Enforcement Agency of asserting a great deal of control over the regulatory process."

For some privacy experts, that's the real question: Is it the FCC's mandate to aid law enforcement? Civil-liberties concerns aside, building a backdoor through which the FBI can monitor communications also inserts a soft spot for hackers. "To the extent that there may be tension in the law," argues the FCC's Knapp, "it's suggested that with that tension in place, the appropriate public interest lies in ensuring that public safety has access to the tools it needed."

There may be more developments to come. In March, the same month the FBI requested that the FCC expand CALEA, the commission released a "Notice on Proposed Rulemaking," which announced plans to look at whether and how the FCC should begin regulating the Internet. Crawford points to its 155th footnote, which says the FCC could, if it wanted to, place tariffs on online newspapers or require that online retailers be able to process 911 emergency calls. "It's sort of a lighthearted footnote," she says. "But for me it suggests the FCC has power over all online services and it's just going to decide what services it's going to act on. This is a turning point in the history of the Internet because telecom agencies all over the world are looking at their very broad enabling statutes and saying 'Someone needs to be in charge of this Wild, Wild West.'" And providers are falling in line with the FCC, she says, because the certainty of regulated business minimizes risk. Or, as an America Online spokesman puts it, "We comply with law-enforcement agencies that bring a legally binding request to us, and we cooperate with them. We've always done that.”

Which is why Crawford says it's time for the FCC, an independent government organization accountable to Congress, to engage in a public discourse if it plans on regulating the Web. "What we need right now is a national conversation about whether and how we're going to regulate Internet services." But even from where she sits, Crawford admits that the question of "whether" is already being answered in the affirmative. It's the "how" that concerns her.

© 2004 Newsweek, Inc.

URL: http://msnbc.msn.com/id/5697267/site/newsweek/